УДК 004.85

В.Н. Соляной, А.И. Сухотерин, Е.Д. Беленко

Россия, г. Королев, Государственное бюджетное образовательное учреждение высшего образования Московской области «Технологический университет»

ЭНЕРГОИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ОБЪЕКТОВ КАК НЕОБХОДИМАЯ ОБЛАСТЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Усложнение задач по обеспечению информационной безопасности в современных условиях является неоспоримым фактом действительности. Принципиально новой задачей в области информационной безопасности (ИБ) следует рассматривать обеспечение безопасности функционирования информационных объектов от скрытых деструктивных энергоинформационных воздействий (излучений) малой интенсивности, исходящих от субъектов (людей), техники и природы. При проявлении резонансных условий данные излучения могут приводить к серьезным нарушениям функционировании современных социотехнических систем. Выявление и разрешение данной проблемы по ИБ в общем виде представлены в материалах статьи.

Ключевые слова: энергоинформационная безопасность, деструктивные воздействия, модель, решения по ИБ.

В современном информационном обществе, в процессе своего бурного развития, начинают проявляться, с одной стороны, странные и, с другой стороны, достаточные опасные и скрытые явления, которые достаточно трудно объясняются или совсем не объясняются традиционной наукой [1,2,3,4,5,6,7,8,9,10,11]. Такие процессы требуют глубокого изучения и учета при обеспечении информационной безопасности защищаемого 186нновационного ресурса на всех уровнях функционирования информационного общества. Именно данная существующая проблема обеспечения информационной безопасности (ИБ) и является предметом обсуждения в данной статье.

В теоретико-прикладном аспекте все объекты информационной защиты следует представлять как сложные социотехнические системы (СТС), включающие три взаимовлияющих друг на друга ключевых компонентов: человек (социум); техника (технические процессы) и окружающая среда (природа). В

этих условиях можно показать существование трех просматриваемых парадигм обеспечения информационной безопасности.

Во-первых, традиционные задачи обеспечения информационной безопасности СТС, в настоящий период времени, реализуются по хорошо разработанной типовой схемы. Данный подход реализуется на уровне достаточно исследуемого процесса по взаимовлиянию материально-вещественных структур и известными физическими полями. При этом такой алгоритм 187нновационно включает в себя: обнаружение и выявление угроз, нарушителей и уязвимостей (с использованием различных инструментальных, как правило, технических средств); определение ущерба (рисков); обоснование и реализация целесообразных мер по противодействию угрозам с оценкой функциональной и экономической их эффективности. Защищаемые информационные 187нновацсы СТС базируются на основе законов классической физики. С учетом изложенного, условно, данный процесс обеспечения ИБ можно представлять как реализация традиционного «материально-вещественного варианта обеспечения информационной безопасности».

Во-вторых, на атомарно-молекулярном (материальном) уроне окружающий мир, включая и СТС, нужно одновременно рассматривать как материальные объекты (в виде большой совокупности взаимовлияющих друг на друга элементарных частиц, находящихся в постоянном движении), так и в виде совокупности излучающих элементарными частицами известных и неизвестных полей (полевой уровень). При этом указанные полевые излучения в обычных условиях существования, как показывают исследования, обладают очень низкой интенсивностью и фактически не фиксируются существующими техническими инструментальными средствами. Такие полевые излучения обладают скрытыми и достаточно высоко проникающими взаимными информационными воздействиями с положительными и деструктивными итоговыми эффектами. Для понимания процессов по обеспечения ИБ современных сложных СТС на полевом уровне можно использовать существующую и достаточно разработанную теорию электронно-магнитных полей на основе одновременного применения принципов классической и квантовой физики. Возможность создания, при определенных внутренних и внешних условиях, в рассматриваемых материально-вещественных объектах естественных или (и) преднамеренных резонансных полевых проявлений и является причиной возникновения достаточно мощных и глубоко проникающих информационно-полевых (типа «электромагнитных») излучений, оказывающих серьезное воздействие на исследуемые информационные процессы и объекты. Данная концепция рассмат-

ривает процессы по ИБ на основе наличия «локального и дистанционных вещественно-полевых воздействий» , т.е. позволяет предполагать возможность наличия целого спектра полевых (типа «электромагнитных») излучений и наличия большого разнообразия различных полевых резонансных эффектов, привязанных к конкретным резонансным частотам. Рассмотренный подход «вариант локально-дистанционного вещественно-полевого обеспечения ИБ» обуславливает необходимость разработки принципиально новой парадигмы обеспечения ИБ уже в настоящее время.

В-третьих, при рассмотрении окружающего материально-вещественного мира с позиций только квантовой физики (на уровне существования элементарных частиц в форме волновых структур) можно предположить, что окружающий мир это единое (комплексное) сложное полевое пространство («единое дальнее информационное поле»), которое существует как совокупность различных всепроникающих слабой интенсивности полевых излучений всех материальных объектов. Данное предположение позволяет предполагать, что материальные объекты могут находиться одновременно и в полевой форме существования, являясь некой волновой структурой «единого информационного поля», одновременно существуя в каждой пространственной точки таково мирового поля (мгновенное распространение изменения информации). Появление в рассматриваемых защищаемых пространствах различных резонансных полевых ситуаций обуславливает возникновения мощных энергетических выбросов с непредсказуемыми эффектами. Условно данный подход рассмотрения обеспечения ИБ можно назвать как «вариант обеспечения безопасности в структуре единого дальнего информационного поля» и требует, уже в настоящее время, приступить к серьезным исследованиям в данной области.

Обобщая вышеизложенные взгляды на обеспечение информационной безопасности современных сложных СТС целесообразно сформировать основные теоретические аспекты сформулированной проблемы в виде концептуальной обобщенной модели [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11]. При этом, 188нновствование различных скрытых полевых излучений окружающего мира можно представить как некие энергоинформационные воздействия, способные оказывать как отрицательные, так и к положительным эффекты на отдельные компоненты и, в целом, на всю СТС. Данное представление рассмотренных ситуаций позволяет утверждать, что в существующей структуре «информационная безопасность» целесообразно ввести новый компонент в виде понятия «энергоинформационная безопасность».

В настоящее время предложенный термин в теоретических исследований в области обеспечения безопасности человека уже ограниченно используется. При этом под «энергоинформационной безопасностью» понимается очень узкое значение, фактически лишь безопасность сознание личности и это очень и очень ограниченный подход данного определения.

В данной работе, под термином «энергоинформационная безопасность (ЭИБ)» соотносится с широким понятием обеспечение безопасности сложных социотехнических систем (взаимно объединяющие и взаимно влияющие компоненты СТС: человек; техника и природа) от скрытых деструктивных энергоинформационных (полевых) излучений малой интенсивности (при условии проявления для них резонансных явлений). Любое физическое тело можно представить как своеобразный резонатор. Данное широкое определение ЭИБ не отрицает существующее понятие и, в тоже время, расширяет данный термин с учетом вышеизложенных позиций.

В соответствии с рассмотренным подходом в данной работе представлены в обобщенном виде целесообразная структура и характеристики основных компонентов предложенной концептуальной модели ЭИБ СТС (рисунок 1).

С учетом вышеизложенного, можно предложить определение основных (ключевых) понятий в области энергоинформационной безопасности (в широком смысле).

Энергоинформационная безопасность (ЭИБ) – это состояние защищенности социотехнических объектов (человека\социума\, технических средств\систем, комплексов\ и природных условий) от малой интенсивности скрытых внутренних и внешних деструктивных энергоинформационных воздействий (ЭИВ);

Цель ЭИБ – исключение (снижение или локализацию) деструктивных энергоинформационных воздействий (угроз) на анализируемые отдельные компоненты или на всю социотехническую систему в целом.

Критерий ЭИБ – адекватное поведение человека (социума), устойчивое функционирование технического компонента и неизменное состояния окружающей среды (природы).

Субъектами ЭИБ являются человек и социум общества (государства), в частности, для отдельных граждан это, прежде всего, их подсознание, а для социума – коллективное их подсознание и которые, в большей своей степени, не контролируются субъектами.

Объектами ЭИБ являются: во-первых, технические компоненты СТС включая и строительные сооружения, обеспечивающие работу субъектов; во-

вторых, природная среда, в которой функционируют все компоненты рассматриваемой СТС.

Содержание других компонентов концептуальной модели ЭИБ представлено на рисунке 1.

Обобщая вышеизложенное можно спрогнозировать роль и место энергоинформационной безопасности в современной информационной войне, которая набирая новые «обороты» усиливает рассмотренные вопросы в виде разработки и использования новых видов информационного оружия. В этих условиях особенно необходимо затронуть вопрос обеспечения энергоинформационной безопасности (защиты) руководителей разных рангов. Все руководители несут личную ответственность как за принимаемые, так и реализуемые решения при наличии сложной информационной обстановки.

Выявление и учет энергоинформационных положительных резонансных воздействий (частот) способствуют на всех этапах управления легче принимать наиболее целесообразные во всех отношениях решения, в частности в интересах:

– подбора кадров (эффективного использования способностей специалистов и совместимости его с коллективом);

– максимального облегчения вопросов планирования и просмотр перспектив развития целесообразных организационных структур (фирмы, организации, предприятия и т. д.);

– просмотра надежности партнеров;

– выбора информационно – энергетически безопасного месторасположения (зданий, помещений, рабочих мест, оборудования, сырья и т.д.);

– выбора наиболее оптимальных тактик и стратегий достижения поставленных целей;

– формирования, в физическом и психологическом смысле, здорового трудового коллектива и т. д.

В настоящее время отсутствует строгое определение термина энергоинформационного поля. Однако, в общем виде, под энергоинформационным полем следует подразумевать пространство, в котором распространяется информация посредством энергоносителя [7]. При этом энергоинформационное поле можно характеризовать:

– мощностью энергии (несущей, принимая в расчет аналогию электромагнитного излучения);

– количество передаваемой информации (степенью стохастически огибающей – количеством гармоник ее спектра электромагнитного излучения, по той же аналогии).

Рисунок 1 – Концептуальная модель энергоинформационной безопасности

С учетом введенного термина, для более подробной характеристики энергоинформационного поля, целесообразно ввести следующие понятия.

2. Энергоинформационная мощность ($Э_t$) и которую можно определить по следующей формуле:

$$Э_t = Э * I, \ [Вт * с * бит], \quad (1)$$

где $Э$ – энергия:

$$Э = Р * t, \ [Вт * с]; \quad (2)$$

P – мощность излучения, Вт;

I – количественная мера информации, бит;

t – время излучения, секунды (с).

2. Плотность энергоинформационного поля (П), под которой следует понимать отношение энергоинформационной мощности к объему пространства (V):

$$П = Э_t / V, \ [Вт * с * бит / м^3], \quad (3)$$

где V – энергия, $м^3$.

3. Для защищаемых информационно-технологических процессов в современных социотехносферных системах очень важна скорость передачи информации, следовательно целесообразно ввести понятие удельная плотность энергоинформационного поля ($П_t$) и под которой понимается отношение плотности энергоинформационного поля ко времени передачи информации:

$$П_t = П / t. \quad (4)$$

С учетом формул (1), (2) и (3) получаем итоговую формулу

$$П_t = [(Э * I) / (V * t)] * k_1 * k_2 * k_3, \quad (5)$$

где k_1, k_2, k_3 – коэффициенты, учитывающие характеристики «приемно-передающих» каналов энергоинформационных излучений, соответственно: человека, техники и природы в рассматриваемых защищаемых социотехносферных информационных объектов.

Из итоговой формулы (5) видно, что удельная плотность энергоинформационного поля ($П_t$) прямо пропорциональна энергии поля ($Э$) и количеству передаваемой информации (I), а также обратно пропорциональна объему пространства (V), где распространяется информация, и времени передачи или приема (t).

Качественная оценка плотности энергоинформационного поля в зависимости от объема сферы рассматриваемого объекта информационной защиты, в которой распространяется деструктивное энергоинформационное воздействие представлена на рис.2.

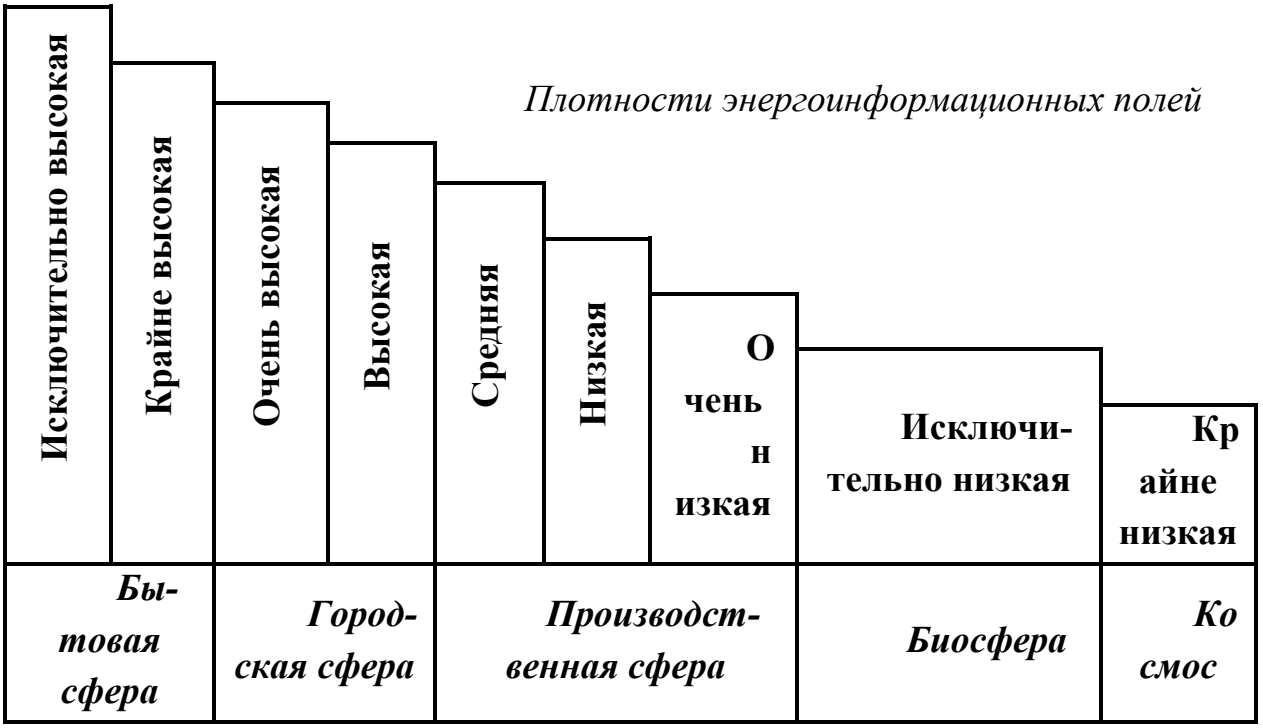

Рисунок 2 – Качественная зависимость плотности энергоинформационного поля от характеристики пространства и его объема

В целом, в данной статье представлена достаточно серьезная область представления существующих на практике деструктивных энергоинформационных воздействий, которые официальная классической наука не отвергает, но и серьезных глубоких исследований не проводит. В тоже время, практические аспекты функционирования современного информационного общества все больше сталкиваются с отдельными фактами из данной области.

В целом, авторы данной статьи считают, что необходимо приступить к глубокому анализу непознанному (скрытому) аспекту области функционирования современных социотехносферных систем. При этом рассмотренную энергоинформационную безопасность (в широком смысле) необходимо рассматривать в сложившейся структуре, прежде всего, как обязательный компонент современной системы обеспечения информационной безопасности нашего государства.

Применение искусственно создаваемых и управляемых энергоинформационных технологий направленных на поражение человека, техники и природы осуществляется скрытно с целью внезапной или постепенной деструкции

(деформации, разрушения) отдельных компонентов современных социотехносферных объектов и может привести к большим потерям в людских, технических и природных ресурсах.

Литература

1. Доктрина информационной безопасности РФ, утверждена Указом Президента Российской Федерации № 646 от 05.12.2016 г.

2. Родионов Б.Н., Титов В.Б., Ярочкин В.И. Энергоинформационная безопасность человека и государства. М.: Паруса, 1997.

3. Павленко А. Р. Защита населения от негативного влияния геопатогенных зон, мониторов, телевизоров. Киев, 1997.

4. Ханцеверов Ф.Р. Эниология. Чудеса без мистики. Книга научных версий. (Книга 2). М., 1999.

5. Соляной В.Н., Сухотерин А.И. Взаимодействие человека, техники и природы: проблема информационной безопасности. Научный журнал (КИУЭС). Вопросы региональной экономики. №5 г. Королев, ФТА, 2010.

6. Рысин Ю. С. Социально –информационные опасности телерадиовещания и информационных технологий. Учебное пособие. М.: Гелиос АРВ, 2007.

7. Перечень специальностей и направлений подготовки высшего образования, соответствующих приоритетным направлениям модернизации и технологического развития российской экономики. Распоряжение Правительства РФ от 6 января 2015 г. №7-р.

8. Соляной В.Н., Сухотерин А.И. Модульно-ориентированный подход формирования базовых дисциплин ФГОС ВО 3+ как основа реализации профессиональной подготовки бакалавров в области информационной безопасности Научно-практический журнал №25, том 2 2015г. «Информационное противодействие угрозам терроризма. Материалы XIX пленума учебно-методического объединения по образованию в области информационной безопасности «Учебно-методическое обеспечение образовательных программ в области информационной безопасности» г. Таганрог, Рост. обл.: Изд-во Южн.фед.унив., 2015.-332 с. ISSN 2219-8792.

9. Соляной В.Н., Сухотерин А.И. Становление направления «Радиоэлектронная безопасность информационных объектов» в системе дополнительного профессионального по информационной безопасности. Научно-практический журнал №25, том 2 2015г. «Информационное противодействие угрозам терроризма. Материалы XIX пленума учебно-методического объединения по образованию в области информационной безопасности «Учебно-методическое

обеспечение образовательных программ в области 195нновационной безопасности» г. Таганрог, Рост. обл.: Изд-во Южн.фед.унив., 2015.-332 с. ISSN 2219-8792.

10. Соляной В.Н., Сухотерин А.И. Практика применения 195нновационного научно-образовательного комплекса по подготовке бакалавров и магистров в области информационной безопасности Научно-практический журнал №25, том 1 «Информационное противодействие угрозам терроризма. **Материалы** XIX пленума учебно-методического объединения по образованию в области информационной безопасности «Учебно-методическое обеспечение образовательных программ в области информационной безопасности» г. Таганрог, Рост. обл.: Изд-во Южн.фед.унив., 2015.-332 с. ISSN 2219-8792.

11. Соляной В.Н., Сухотерин А.И, Шихнабиева Т.Ш., Сиротский А.А. Некоторые элементы ассоциативности в методиках преподавания дисциплин технической направленности. Организация менеджмента информационной безопасности в финансово-кредитных учреждениях. Информационная безопасность бизнеса и общества. Сборник статей научно – преподавательского состава кафедры информационных систем, сетей и безопасности / Российский Государственный Социальный Университет. – М.: Издательство «Перо», 2016.-111 с. ISBN 978-5-906851-15-4